Alan Himmelfarb - SBN 90480
KAMBEREDELSON, LLC
2757 Leonis Boulevard
Vernon, California 90058
Telephone: (323) 585-8696

Joseph H. Malley - TX SBN: 12865900
LAW OFFICE OF JOSEPH H. MALLEY, P.C.
1045 North Zang Boulevard
Dallas, Texas 75208
Ph. (214) 943-6100
Fax (214) 943-6170

Counsel for Plaintiffs

ORIGINAL
FILED
FEB 27 2009
RICHARD W. WIEKING
CLERK, U.S. DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
OAKLAND

E-filing

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA

MMC

SUSAN SIMON, individual, on behalf of herself and all others similarly situated,

Plaintiffs

v.

ADZILLA, INC. [NEW MEDIA], a Delaware Corporation; CONDUCIVE CORPORATION, a Delaware Corporation; CONTINENTAL VISINET BROADBAND, INC., a Delaware Corporation; CORE COMMUNICATIONS, INC., d/b/a CORETEL COMMUNICATIONS, INC., a Delaware Corporation; AND JOHN DOES 1-50, Corporations Defendants.

Defendants.

CASE NO. C09-00879

ADR

JURY DEMAND

COMPLAINT FOR:

1. Violation of Electronic Communications Privacy Act, 18 U.S.C. § 2510;
2. Violation of Computer Fraud and Abuse Act, 18 U.S.C. § 1030;
3. Violation of California's California Invasion Of Privacy Act,, California Penal Code § 630;
4. Violation of California's Computer Crime Law, Penal Code § 502;
5. Aiding and Abetting;
6. Civil Conspiracy;
7. Unjust Enrichment

CLASS ACTION COMPLAINT

Plaintiff Susan Simon, on behalf of herself and all others similarly situated, by and through her attorneys, KamberEdelson, LLC, and the Law Office of Joseph H. Malley, P.C., as and for her complaint, alleges as follows upon information and belief, based upon, inter alia, investigation conducted by and through her attorneys, which are alleged upon knowledge, sues Defendants Conducive Corporation, Adzilla, Inc. [New Media],, Continental VisiNet Broadband, Inc., Core Communications, Inc., d/b/a CoreTel Communications, Inc., and John Does 1-50, corporations and states:

NATURE OF THE ACTION

1. This is a class action lawsuit brought by and on behalf of similarly situated internet users whose privacy and computer security rights were violated by the undisclosed and unconsented to interception, Deep Packet Inspection and copying and/or alteration of their internet communications.

2. The following parties, jointly and severally, engaged in a scheme to spy-for-profit on the internet communications of unwitting internet users:

(a) Conducive Corporation, a corporation doing business in online behavioral advertising, owner of AdZilla New Media, Inc.;

(b) AdZilla New Media, Inc. (hereinafter referred to as "Adzilla"),

(c) Adzilla Affiliated Competitive Local Exchange Carriers ("AACLECs") including Core Communications, Inc., d/b/a CoreTel Communications, (hereinafter referred to as "CoreTel"), and;

(d) Adzilla Affiliated Internet Service Providers ("AAISPs"), including Continental VisiNet Broadband, Inc., doing business with CoreTel, and/or other Competitive

Local Exchange Carriers.

3. The parties identified and described in Paragraph 2, above, knowingly authorized, directed, ratified, approved, acquiesced, and/or participated in the intentional interception of the plaintiff's and other ISP subscribers' (class members') online transmissions, without the authority or consent of the plaintiff or other ISP subscriber class members using Deep Packet Inspection ("DPI"). Deep Packet Inspection, when implemented at the ISP or CLEC level, allows a third party to access, view, and, on information and belief, copy and retain *all* details of *all* communications between a subscriber and the internet, including those communications both sent by the subscriber or received by the subscriber from any location on the internet.

4. Deep Packet Inspection of internet communications accesses, acquires, and discloses sensitive information ("SI"), personal identifying information ("PII"), personal information ("PI"), and non-personal indentifying information ("Non-PII"). The Deep Packet Inspection, as described more fully herein below, was made possible through the utilization of an Adzilla device referred to as a "Zillacaster," installed at either the ISP infrastructure, or at the Competitive Local Exchange Carrier infrastructure. All of this was accomplished without any notice to and without any consent obtained from the plaintiff or any ISP subscribers.

5. Excluded from this action are:

(a) Any corporations that affiliated with Conducive or Adzilla, but did not activate Adzilla devices, products, and/or services to intercept online transmission of ISP subscribers;

(b) Any Adzilla Affiliated Competitive Local Exchange Carriers, who did not activate Adzilla devices, products, and/or services to intercept online transmission of internet end-users;

(c) Any Adzilla Affiliated Internet Service Provider wherein the Adzilla devices, products, and/or service was activated to intercept online transmission of ISP subscribers without the knowledge and/or consent of the ISP.

(d) Any Adzilla Affiliated Competitive Local Exchange Carriers wherein the Adzilla devices, products, and/or service was activated to intercept online transmission of ISP subscribers without the knowledge and/or consent of the CLEC.

6. The class action period (the "Class Period"), pertains to the period that Adzilla appliance was first activated, operational, and intercepting internet subscriber communications, to the date Adzilla and/or any of the Competitive Local Exchange Carriers, including CoreTel and/or any of the AAISPs finally deactivated the Adzilla appliances, a period that roughly approximates on or about June 1, 2007 to October 1, 2008.

7. The conduct of Conducive, Adzilla, CoreTel, Continental Broadband, and the Doe AACLECs and Doe AAISPs, individually and jointly, constituted one (1) or more of the following:

- Violation of Electronic Communications Privacy Act, 18 U.S.C. § 2510;
- Violation of Electronic Communications Privacy Act, 18 U.S.C. § 2702;
- Violation of Computer Fraud and Abuse Act, 18 U.S.C. § 1030;
- Violation of California's California Invasion Of Privacy Act, California Penal Code § 631;
- Violation of California's Computer Crime Law, Penal Code § 502.

JURISDICTION AND VENUE

8. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332. The aggregate claims of plaintiff and the proposed class members exceed the sum or value

of $5,000,000.00.

9. Conducive Corporation is a Delaware corporation which maintains its headquarters at 55 Broad Street, Floor 23, New York, New York 10004 and is a citizen of the states of Delaware and New York.

10. Adzilla, Inc. is a Delaware corporation with its U.S. headquarters in San Mateo, California and is a citizen of the states of Delaware and California. Plaintiff is a citizen and resident of Virginia, and asserts claims of behalf of a proposed class whose members are scattered throughout the fifty states (including the 49 states besides California) and the U.S. territories. There is minimal diversity of citizenship between proposed class members and the Defendant.

11. This Court also has personal jurisdiction over defendants because (a) a substantial portion of the wrongdoing alleged in this complaint took place in this state; (b) defendant Adzilla's principal place of business is located in this state; and (c) defendant is authorized to do business here, has sufficient minimum contacts with this state, and/or otherwise intentionally availed itself of the markets in this state through the promotion, marketing, and sale of its product in this state, to render the exercise of jurisdiction by this Court permissible under traditional notions of fair play and substantial justice.

12. Venue is proper in this District under 28 U.S.C. §1391(b) and (c). A substantial portion of the events and conduct giving rise to the violations of law complained of herein occurred in this District; defendant Adzilla's principal executive offices and headquarters are located in this District at 1000 Marine Boulevard, Suite 105, Brisbane, CA 94005; and defendant conducts business with consumers in this District.

13. This Court has personal jurisdiction over Defendants Conducive and Adzilla under Cal. Code Civ. Proc. § 410.10 because Adzilla, maintains its corporate headquarters in, and the acts alleged herein were committed in California. All of the acts alledged in this complaint against Adzilla were undertaken with the knowledge, support, and assistance of Defendant Conducive.

14. The following corporations are citizens of states other than California; however, acts upon which liability is alleged herein were committed by the corporations listed in this paragraph in the state of California:

1. Core Communications, Inc. d/b/a CoreTel Communications, Inc.;
2. Continental VisiNet Broadband, Inc;
3. Adzilla Affiliated Competitive Local Exchange Carrier Does 1-25;
4. Adzilla Affiliated Internet Service Provider Does 26-50.

The conduct complained of involved the interception, copying, transmission, collection, storage, usage, and altering of personal, private data of the class members. This conduct was devised, developed, implemented, and directed from within this judicial district in California. The actual information and data from each of the AAISP Subscribers and Competitive Local Exchange Carriers was, without exception, transmitted to Adzilla in California. Therefore, substantial, if not all evidence of wrongdoing as alleged in this complaint is located in this judicial district.

INTRADISTRICT ASSIGNMENT

15. Defendant Adzilla Inc.'s principle United States executive offices and headquarters are located in this District at 1000 Marina Boulevard, Suite 105, Brisbane, CA 94005. Intra-district assignment to the Oakland or San Francisco Division is proper pursuant to Local Civil Rule 3-2(d).

PARTIES

16. Plaintiff Susan Simon ("Simon"), is a citizen and resident of Richmond, Virginia, (Chesterfield County). At all relevant times herein, Simon was a subscriber to Continental VisiNet Broadband, Inc., an internet service provider.

17. Defendant Conducive Corporation (hereinafter "Conducive"), parent company of Adzilla New Media, Inc., is a Delaware corporation which maintains its headquarters at 55 Broad Street, Floor 23, New York, New York 10004. Defendant Conducive does business throughout the United States, and in particular, does business in State of California and in this County.

18. Defendant Adzilla [New Media], Inc. (hereinafter "Adzilla"), is a Delaware corporation which maintains its headquarters at 1000 Marina Boulevard, Suite 105, Brisbane, California 94005. Defendant Adzilla was acquired by and became a subsidiary of Conducive Corporation as of May 3, 2006. Defendant Adzilla, Inc., does business throughout the United States, and in particular, does business in State of California and in this County.

19. Continental VisiNet Broadband, Inc., (hereinafter "Continental Broadband"), is a Delaware corporation which maintains its headquarters at 253 Monticello Avenue, Suite 200, Norfolk, Virginia 23510. Defendant Continental Broadband does business throughout the United States, and in particular, transacted business in State of California and in this County. Defendant Continental Broadband knowingly and expressly allowed, permitted, aided, encouraged, and assisted in:

- the interception, copying, transmission, and alteration of personal, private data of internet subscribers to this county in the state of California;
- the copying collection, storage, usage, of personal, private data of internet subscribers

in this county in the state of California; and

- the usage, alteration, and transmission of data from this county in the state of California.

20. Defendant Core Communications, Inc. d/b/a CoreTel Communications, Inc., (hereinafter "CoreTel Communications"), is a Delaware corporation which maintains its headquarters at 209 West Street, Suite 302, Annapolis, Maryland, 21401. Defendant CoreTel Communications does business throughout the United States, and in particular, transacted business in State of California and in this County. Defendant CoreTel Communications knowingly and expressly allowed, permitted, aided, encouraged, and assisted in:

- the interception, copying, transmission, and alteration of personal, private data of its subscribers to this county in the state of California;
- the copying collection, storage, usage, of personal, private data of its subscribers in this county in the state of California; and
- the usage, alteration, and transmission of data from this county in the state of California.

21. On August 2, 2007, Adzilla Inc., released a press release entitled "Adzilla Secures $10.25 Million in Series A Funding - Proceeds Will Be Used to Continue to Expand Its Leadership in the Market for Behavioral Targeted Online Advertising." The press release stated, in pertinent part: "Since its founding in 2004, Adzilla has completed product development and successfully deployed its product with eight (8) internet service providers."

22. In an article entitled "Conducive Acquires Tracking Company" published by MediaPost on May 4, 2006, the article cited statements by Conducive CEO Jim Waltz and Robert Roker, AdZilla's chief technology officer, stated in part:

> ZillaCastingT works with hardware installed on-site at an Internet service provider. So far, Conducive has signed up 16 ISPs to use the device, including regional ISPs like Champion and Millennium. Sixteen of the top 30 publishers by ad traffic have also been signed, Waltz said; he declined to name any of the companies.

http://www.mediapost.com/publications/index.cfm?fa=Articles.showArticle&art_aid=42986

23. Defendants, Adzilla Affiliated Competitive Local Exchange Carrier Does 1-25, are corporations similarly situated to CoreTel in that they knowingly aided, assisted, directly participated in, and/or acquiesced in the conduct complained of herein. The contractual obligations of Adzilla may require Adzilla to provide notice to the Competitive Local Exchange Carrier Does of this matter so as to appear and protect their interests, or these Competitive Local Exchange Carrier Does may provide notice to confirm their Adzilla Program activity independent of Adzilla. In either case, when the identity of these Competitive Local Exchange Carrier Does 1-25 who are sued as Doe defendants are identified, Plaintiff will amend their complaint to name such parties as Competitive Local Exchange Carrier defendants.

24. Defendants, Adzilla Affiliated Internet Service Provider Does 26-50 aided, assisted, directly participated in, and/or acquiesced in the conduct complained of herein. The contractual obligations of Adzilla may require Adzilla to provide notice to the Adzilla Activated ISP Affiliates of this matter so as to appear and protect their interests, or these Adzilla Activated ISP advertisers may provide notice to confirm their Adzilla Program activity independent of Adzilla. In either case, when the identity of these Adzilla Activated ISP advertisers who are sued as Doe defendants are identified, Plaintiff will amend their complaint to name such parties as Adzilla Activated ISP Affiliate defendants.

STATEMENT OF FACTS

25. The basis of this action involves commercial joint ventures between Adzilla, an

online behavioral advertiser, competitive local exchange carriers (CLECs), and internet service providers ("ISPs"); wherein an Adzilla appliance, referred to as a "Zillacaster," is installed into the ISP and/or CLEC network in order to intercept the clickstream data of internet end-users, without their knowledge or consent, and sold to third parties for advertising purposes.

26. The "Zillacaster" is the name given by Adzilla to a device that, in essence, taps into the communication stream between the subscriber and the internet. Without any notice whatsoever to the internet user, the Zillacaster oversees, inspects, copies, transmits, and even permits the alteration of the internet subscriber's internet communications – secretly, without any hint that the communications are being monitored, let alone altered. A Zillacaster intercepts and copies all data passing through the data pipe to which it has been affixed.

27. The Zillacaster device needs to be installed into the internet communication data stream at specific locations in order to be able to capture the internet communications of individually identifiable users. The cooperation and collaboration of the Internet Service Provider ("ISP"), and/or the Competitive Local Exchange Carrier ("CLEC") is an essential element in the scheme to intercept and monitor the internet communications of end-users.

28. The Competitive Local Exchange Carriers ("CLEC") provide the main regional pipes through which internet connections are provided to the public. The CLECs, in turn, sell local internet connection services to ISPs. The ISPs then resell internet connections to individual users and businesses. There are certain points in these connections where all data from specific consumers or companies must pass. The CLECs and the ISPs physically control those points of data interception. Thus, in order for the Zillacaster to engage in its scheme of interception, monitoring, and altering of data, the CLECs and the ISPs must knowingly aid, acquiesce, assist, and participate in the process by which the Zillacaster gains access to the data streams which the

CLECs and ISPs control.

29. Paul Ohm, Associate Professor of Law, Computer Crime Law, Information Privacy, Criminal Procedure, Intellectual Property, University of Colorado Law School observed:

> **The Greatest Threat to Privacy: The Internet Service Provider**
>
> I have recently posted on SSRN the article that ate my summer, *The Rise and Fall of Invasive ISP Surveillance*. I make many claims in this article, but the principal one, and the one I want to spend a few posts elaborating and defending, is found in the first sentence of the abstract: "Nothing in society poses as grave a threat to privacy as the Internet Service Provider (ISP)." In this first post, let me explain why ISPs pose an enormous threat to privacy:
>
> Simply put, your ISP has the means, motive, and opportunity to scrutinize nearly every communication departing from and arriving to your Internet-connected computer:
>
> **Opportunity:** Because your ISP serves as the gateway between your computer and the rest of the Internet, every e-mail message, IM, and tweet you send and receive; every web page and p2p-traded file you download; and every VoIP call you place travels first through your ISP's routers.
>
> **Means:** A decade ago, your ISP lacked the tools to efficiently analyze every communication crossing its network, because computers were relatively slow and networks were relatively fast. I use the analogy of the policeman on the side of the road, scrutinizing the passing cars. If the policeman is slow and the road is wide and full of speeding cars, the policeman won't be able to keep up.
>
> Over the past decade, while network bandwidth has increased, computer processing power has increased at a faster rate, and your ISP can now analyze more information, more inexpensively than before. The roads are wider today, but the policemen are smarter and more efficient. An entire industry--the deep-packet inspection industry--has arisen to provide hardware and software tools for massive, widespread, automated surveillance.
>
> **Motive:** Third-parties are placing pressure on ISPs to spy on users in unprecedented ways. Advertisers are willing to pay higher rates for behavioral advertising. For example, Ikea will pay more to place an ad in front of people who have been recently surfing furniture websites. To enable behavioral advertising, companies like Adzilla and Phorm have been trying to convince ISPs to collect user web-surfing data they do not collect today. Similarly, the copyrighted content

> industries seem willing to pay ISPs to detect, report, and possibly block the transfer of copyrighted works.
>
> **Paul Ohm; September 03, 2008**
> http://www.concurringopinions.com/archives/2008/09/the_greatest_th_1.html

30. The "Zillacaster" is just such a device as described by Paul Ohm for the Deep Packet Inspection ("DPI") of the ISP subscriber's clickstream data in order to monetize such data for commercial advertising.

The Internet Service Provider

31. Consumers access the internet though an Internet Service Provider ("ISP"). Whether the ISP offers internet connectivity through dial-up; DSL (typically Asymmetric Digital Subscriber Line, ADSL); broadband wireless; cable modem; fiber to the premises (FTTH); or Integrated Services Digital Network (ISDN), the ISP is the 'gateway' through which all consumer and business communications must pass in order to take advantage of the benefits of the internet. All email sent by the end-user is routed through the ISP in order to be delivered to its ultimate recipient. All web-based interactions similarly are routed from the user's computer through the ISP and passed along to the relevant website. All communications from any website to the end-user must pass though the ISP. Anything that the end-user does that involves the internet passes through the conduit that the ISP provides. ISPs are allowed, within their normal course of business as a necessary incident to the rendition of their services, to inspect a subscriber's datastream for reasons such as: viruses, spam, searching for non-protocol compliance, securing their network, police bandwidth, and maintain the overall "health" of their network; however conducting Deep Packet Inspection for subscriber content is not within those rights.

32. ISPs require subscribers to consent to an Acceptable Use Policy when they

initially subscribe to their services. None of the Acceptable Use Policies of the defendant ISP's specifically provided details concerning the interception, monitoring, copying and alteration of their online communications for sale to advertisers.

The Competitive Local Exchange Carrier (CLEC)

33. A Competitive Local Exchange Carrier (CLEC) is a telecommunications provider company (sometimes called a "carrier") that competes with other, already established carriers (generally the incumbent local exchange carrier (ILEC). CLECs evolved from the Competitive Access Carriers (CAPs) that began to offer private line and special access services in competition with ILECs beginning in 1985. The CAPs deployed fiber optic systems in the central business districts of the largest US state public utility commission competitions. By the early 1990's, the CAPs began to install switches in their fiber systems. By the mid-1990s most of the large states had authorized local exchange competition. The Telecommunications Act of 1996 incorporated the successful results of the state-by-state authorization process by creating a uniform national law to allow local exchange competition.

34. A CLEC is a telephone company regulated by the same rules and regulations as the local operating company presently serving the community. It is a Competitive Local Exchange Carrier in competition with the ILEC or Incumbent Local Exchange Carrier (usually the Regional Bell Operating Company (RBOC) or other Independent Telephone Company such as Verizon, Sprint, Ameritech, etc). The CLEC offers the same type of services to its customers as previously provided by the ILEC. As used herein for all purposes of this Compliant, the term "CLEC" includes *any* Local Exchange Carrier, whether it is a CLEC ,or an ILEC, or *any other carrier* that provides internet services directly to the public or for resale to ISPs, if such carriers were involved in the utilization of an Adzilla Zillacaster or other Adzilla device for the

interception and monitoring of end-user communications.

35. Some ISPs require the involvement of a Competitive Local Exchange Carrier ("CLEC"), such as CoreTel, to accomplish their task of providing internet to the ISP subscribers.

Traditional Online Advertising Model

36. Traditionally, advertising on websites evolved based upon the business model used by the newspaper industry, in that they relied on traditional advertising in order to provide content to their subscribers at a reduced rate for the cost of the content. Subscribers would read the content and advertisers hoped their ad would attract the reader.

37. Commercial websites use online advertising in order to promote content to the consumers without charge and require online advertising to support this objective. Commercial websites, known as "publishers" allow portions of their web page to be sold to online advertising networks, which act as an intermediary between "publishers" and the "advertisers."

38. As technology advanced, publishers then desired to identify and track users while they were on their site; therefore "first party" tracking devices, referred to as "session cookies," were implemented. Cookies were a parcel of text sent by a publisher server to the user's browser, so that the user could be identified during the session when they re-entered and navigated the publisher's site.

39. Online advertising companies then desired a "tracking system" to gauge their advertising activity while the user navigated online in and out of their ad networks, and "persistent cookies" or "third-party cookies" accomplished this goal.

40. In order to monopolize the online advertising industry, online advertising companies created a network of publishers, "ad network," linked by a common ad server. Third-party cookies feed into the clickstream data of the consumer by the publisher and/or ad network

providing the ability to monitor the consumer's online activity.

41. The online advertising industry then sought to maximize the "relevance" of ad placement which could provide benefit to the users' interest, thus there developed two advertising models to analyze consumer's interest: "Contextual Advertising" and "Behavioral Advertising."

42. Contextual Advertising matched ads to the content of the webpage the consumer was viewing. For example, if the consumer was visiting a car site, which was within the ad network of sites, car ads would be placed on that site for the consumer to view.

43. Contextual Advertising was flawed since periodic online searches by users provided temporary limited interest.

44. Behavioral Advertising analyzed the consumer's interest over a period of time, attempting to gauge a pattern of behavior relating to online searches. If the consumer was visiting multiple car sites over a period of time, and then searched for a sports site, car ads would appear on the sports site.

45. Online Behavioral Advertising networks created a digital dossier of consumers by tracking their online activities on publisher sites within their network.

46. Online advertisements, targeted or otherwise, were disfavored by consumers. As software programs that filtered online activity and deleted browser cookies developed in sophistication and availability, the consumer gained control over advertising strategies and advertiser attempts at data collection. Without the ability to maintain the accurate collection of user data, online advertising, contextual or behavioral, was not accurate.

47. The ultimate goal for online advertising networks became to obtain a complete digital dossier of all consumers, including all data pertaining to their sensitive identifying

information ("SII"), personal identifying information ("PII") and non-personal indentifying information ("Non-PII"). The only restraints to achieving this objective were governmental regulatory bodies, privacy laws, and consumer backlash.

A. Deep Packet Inspection "DPI"

48. The Internet consists of a network of inter-connected computers in which data are broken down into small, individual packets and forwarded from one computer to another until they reach their destinations.

49. A packet can be thought of as a Russian nesting doll. Packets are built up in successive layers of information -- each one wrapped around all of the "inner" layers that have come before through a process called encapsulation. The innermost layer is usually what is considered to be the "content" of the message—such as the body of the e-mail message or the digital photograph being downloaded from the web. Outer layers contain a number of things that are non-content—such as the addresses used to deliver a message (although outer layers may include content as well).

50. Shallow Packet Inspection might provide information on the origination and destination IP addresses of a particular packet, and it can see what port the packet is directed towards.

51. Deep Packet Inspection, however, looks at the payload of the packet – the actual content of the communication. Whereas Shallow Packet Inspection might reveal a consumer accessing a travel related website, Deep Packet Inspection would reveal the travel destination, whether the consumer was comparing prices, or buying a ticket, how many people were traveling, what they paid, and the credit card information used to make the payment.

B. The Device

52. On October 10, 2007, the International Internet Marketing Association presented a conference entitled “Behavioral Targeting – Beating Banner Blindness” in Vancouver, Canada. Robert Roker, CTO of Adzilla New Media was one of the two presenters at that conference. Mr. Roker’s presentation was described by the conference organizer as follows :

> "ADZILLA Improves the delivery of online advertising in ways that benefit all stake holders within today's ad-ecosystem"
> ADZILLA will discuss how Service Providers (Telecommunications, Cable Companies, ISPs, Wireless Companies) have been locked out of participating in the delivery of online advertising. Today, Providers use their network pipes to process all online advertising but don't get paid. This is mostly because they don't add any decision making or relevancy when delivering and advertisement. Their network pipes observe their subscriber's browsing stream, they have access to information they know about their own subscriber records, and provision services to precise geographic locations.
> ADZILLA introduces a technology called ZILLACASTING a network device installed right inside the Service Provider's environment. It takes the guesswork out of analyzing user behavioral trends because it can identify each user session, process their complete browsing stream, and in real-time offer to Advertiser's, Agencies, Rep Firms, or Ad Networks the ability to suggest alternate ad propositions. This all done without revealing private information of any sort.
> Our behavioral targeting called RELEVANCY AI, collects more than 6,000 detailed types of trending. These opportunities are centric to the user's browsing session and not necessarily the specific website being viewed. Instead of placing the advertisement on a premium website, the system may negotiate a better cost on the next website visit, perhaps only seconds later at half the price.
> In this presentation we will show how our proposition benefits the entire ad-ecosystem by:
>
> 1. allowing the end-user to receive better ad content without the use of cookies or spyware
> 2. the Service Provider to generate new revenue while maintaining strict compliance to privacy
> 3. the advertiser to acquire ultra-premium ad targeting with less waste and lower costs
> 4. the website owners to monetize their advertising spots on pages at higher yields
>
> This is a win win for all

https://www.iimaonline.org/page/events/ezlist_event_B40975C6-82D2-4FFC-89DF-182926575C1A.aspx

53. What Mr. Roker was describing was, of course, the real-time interception,

monitoring, recording, analysis, and altering of an individual's internet browsing activities.

54. A patent registered by Adzilla in 2007, with Robert Roker as inventor, states in relevant part:

> PATENT INFORMATION
>
> India Patent:
> BigPatents India
> "METHOD AND SYSTEM OF TARGETING CONTENT"
> Application: 6769/DELNP/2007 A, Filing date: 2007-08-31, Publication date: 2007-12-14
> Applicant: 1)ADZILLA, INC.
> Inventor: 1) ROKER, ROBERT
>
> ZILLACASTING
> Goods and Services: IC 009. US 021 023 026 036 038. G & S: Computer software for monitoring and modifying data transmitted over the Internet, wide area networks and local area networks
> IC 035. US 100 101 102. G & S: Advertising services, namely, placing advertisements on the Internet for others by modifying web site content to display such advertising, advertising agency services, dissemination of advertising for others via the Internet and rental of advertising space
> IC 042. US 100 101. G & S: Computer services, namely, monitoring, analyzing, and reporting on Internet and network traffic and data for determining demographic and behaviorally targeted information

55. The Zillacaster is an appliance that was purpose-built (hardware and software) to peer deep inside the flow of data from specifically identifiable internet users. From the vantage point of the ISP or CLEC, the appliance was well positioned so that in either direction, the content data stream could be monitored and redirected through the Zillacaster and encoded/decoded for the purpose of tailoring the requested/delivered content to the user. In other words, the Zillacaster had the built-in capacity to permit the alteration -- the addition, removal, or blocking -- in real time – of the content that the internet user was viewing.

56. In an online article by Zachary Rodgers, at ClickZ Network entitled "Toby Gabriner to Helm ISP-Based Behavioral Ad Firm Adzilla" dated January 29, 2008, the article states, in part:

> "As CEO of Adzilla, Toby Gabriner will hold the reins of a company that aims to help Internet service providers **collect data on the online activity of their subscribers,** then use that data to serve ads to them on the wider Web. The approach is fairly new, but already some half dozen vendors have emerged to support it -- firms with names like NebuAd, FrontPorch and Project Rialto. Hundreds of ISPs are rumored to be considering the practice, and several -- including CenturyTel -- have already conducted regional tests.
> **"This is the last bastion, or the last mile, of behavioral targeting,"** Gabriner told ClickZ. "**There's not much closer to the end user that you can get.** From that perspective it's a very interesting and exciting opportunity."
>
> **He acknowledged the privacy worries some have expressed about near-total data collection on individual Internet users.** These include concerns that ISPs and their vendors may accidentally collect personally identifiable information and that user-centric behavioral tracking could lead to a customer backlash. (Emphasis added.)

http://www.clickz.com/3628256

57. Adzilla obtained its data by tapping directly into the consumer's internet connection, either at the ISP or CLEC level. With cooperation and participation of the named Defendants, Adzilla placed a hardware interception device directly into the data hub of either the ISP or the CLEC. Each device can monitor all of the information going to and from users. Multiple devices are used to insure capture of all data transmitted between the consumer and the internet. The device associates the information it sees with the identity of a particular user, along with uniquely identifying information about a users' computer in order to identify the particular consumer whenever the user should sign on to the internet at a later session, in order to maintain a complete and up-to-date dossier on the individual user. The Defendant ISPs'/ CLECs routed all of their customers' traffic; therefore each was in a uniquely perfect vantage point from which to monitor all the traffic to and from a consumer using Deep Packet Inspection (DPI).

58. The ZillaCasting software was designed to be "stealth" -- not detectable. Zillacasting is basically a "transparent tracking proxy," not the usual transparent proxy.

59. In computer networks, a proxy acts as a go-between, or "middleman," which

when installed acts to intercept the data flow between the internet user and the web. Thus, the proxy passes communications between the internet user and the web to accomplish a task that has benefits with indirect communications over direct communications. Proxies are commonly used in enterprises so that many private IP addresses can share a public IP address and/or so that certain frequently-demanded content is cached locally for speed and bandwidth savings. Some proxies are also used by users to "placeshift," to mask identity, or to bypass a network block or other network issue. A user allows the actions of a proxy by configuring the proxy address in settings, or choosing software or settings that enables and responds to proxy auto configuration.

60. In each of the above described implementations of proxy technology, the internet user or server owner has knowledge and control over the use of a proxy. In Adzilla's case, however, the Zillacaster diverts communication within the ISP's network without the knowledge of the end-user, and without regard to the end-user's configuration of their browser, software choices and precautions. The activation of the Zillacaster serves as a "hostile proxy."

61. In normal use of a transparent proxy, the user requests pages/site through the proxy so the site does not know who is requesting it. In the case of the Zillacaster, the user has no part in setting up their access to use a proxy. The ISP and/or CLEC put the proxy in place, without the end user's knowledge, and all of the user's access went through that proxy.

62. When using a regular proxy, the communication path between end hosts is to the designated proxy server, and nothing is impersonated. Adzilla's proxy, however, is purposefully designed to appear to the subscriber that the subscriber is communicating directly with the host web page's actual host. In fact, when the Zillacaster is in operation, the subscriber is communicating directly with the Zillacaster, impersonating the host. This is fraud.

63. Customer consent is not sought, and it is never obtained. Adzilla, in concert with

the ISP and the CLEC, have intentionally configured the Zillacaster system to keep internet subscribers completely in the dark that any proxy is being used at all. As a result, the Zillacaster is able to achieve an almost perfect snooping capability – seeing everything the internet subscriber sees, noting every click, recording every action, reporting every purchase and economic decision, all without any notice of warning that everything the subscriber does on the internet is being observed and recorded.

64. On May 3, 2006, in an Adzilla press release entitled; "Conducive Corporation Completes Acquisition of AdZilla New Media," Jim Waltz, Conducive's Chief Executive Officer stated: "Combined with our adMarketplace(TM) targeted audience delivery system, Zillacaster allows us to dynamically transfer each ISP subscriber's online DNA to publishers and ad networks on demand . . ." The reference to the "DNA" of each ISP subscriber" is not mere puffery – the Zillacaster allowed Adzilla to obtain the most intimate, private, and incredibly detailed dossier on each and every individual subscriber whose data passed through its spying device. As long as the device was active, every single view, click, action, and transaction by an internet user was secretly, comprehensively, and permanently recorded and communicated to Adzilla at its California headquarters.

Facts Pertaining To The Interception Of Plaintiff's Data

65. At all times relevant to the allegations contained in this complaint, Plaintiff Susan Simon ("Simon" or "Plaintiff") was a subscriber to Continental VisiNet Broadband, Inc., an Internet Service Provider.

66. In June 2007, Plaintiff Simon observed that her host ISP was assigning her a range of IP addresses which differed from previously assigned addresses. Following up with a DNS lookup on June 14, 2007, Plaintiff Simon found that she had been assigned a new host

name: ash0101m101.adzilla.com. Accompanying this new host name were several crawler/server entries which were entirely unfamiliar to the plaintiff. These entries showed that, beginning on June 12, 2007, the entries accessed a hidden script on her domain server. The logs showed that the referrer indicated that these entries emanated not only from plaintiff's computer, but from the Plaintiff personal homepage. In essence, an outside entity, one with which plaintiff was entirely unfamiliar, was accessing and searching plaintiff's web log activities, but identifying itself as having originated from plaintiff's own unique homepage.

67. Further research revealed that, every time plaintiff logged in to the internet, regardless of how or through which means she logged in, she was assigned the same IP address – one which was registered to Adzilla. This information did not show up on an ordinary IP search, but only when the plaintiff sought a record of her IP address through a proxy. In other words, the Adzilla IP address assignment was intended to be deliberately concealed from plaintiff.

68. Plaintiff Simon made inquiries to Adzilla regarding these unauthorized events. Plaintiff Simon also made inquiries to her ISP.

69. Plaintiff Simon was never apprised that her IP address would be changed from her originating ISP to and Adzilla-based IP address. Plaintiff Simon never consented to this change in the terms of her ISP subscriber agreement.

70. Plaintiff Simon was never apprised that her web-based internet actions would be subject to tracking and information collection activities, by Adzilla or anyone else. Plaintiff Simon was never apprised that information so collected would be sold by Adzilla, or anyone else, for behavioral marketing purposes.

71. Plaintiff Simon never gave her consent for her web-based internet actions to be subject to tracking and information collection activities, by Adzilla or anyone else. Plaintiff

Simon never gave her consent for information collection to occur regarding her web-based internet actions, nor did she give consent for such collected information to be sold by Adzilla, or anyone else, for behavioral marketing purposes, or any other purposes.

72. Plaintiff Simon's internet service provider Continental Broadband, provided the following privacy / terms of service statement:

> **Privacy Policy of Continental Broadband**
> **Our Commitment To Privacy**
> Your privacy is important to us. To better protect your privacy we provide this notice explaining our online information practices and the choices you can make about the way your information is collected and used. This notice applies to all information collected via the Continental Broadband website.
>
> **The Way We Collect and Use Personal Information:**
> Personal information is not requested or required by the Continental Broadband website. We only collect information that you provide when you send us an email. We use the information you provide about yourself or your company to respond to your inquiries or to provide information about our products and services. We do not share this information with outside parties except to the extent necessary to fulfill any orders you may place or as may be required by law.
> We may also use non-identifying and aggregate information to better design our website and products. However, we do not use "cookies" on our website at this time.
>
> **Our Commitment To Data Security**
> We use industry standard security procedures to prevent unauthorized access, maintain data accuracy, and ensure the correct use of personal information under our control.

Jurisdictional Facts Related to the Intercepted Data

73. At all times relevant to the allegations contained in this complaint, Adzilla's data analysis center, where all of the user's intercepted internet data was transmitted to from Adzilla's device with the assistance of the AAISPs and CLECs, was located in the state of California.

74. At all times relevant to the allegations of this complaint, Adzilla's ad servers where all of the intercepted internet data was collected, stored, and processed was located in the

state of California.

75. At all times relevant to the allegations of this complaint, Adzilla's headquarters where its ad networks functioned in order to associate with websites that wished to host advertisements and advertisers to run on users' webpages was located in the state of California.

76. At all times relevant to the allegations of this complaint, all intercepted internet data was transported to, and continues to remain within the Adzilla's headquarters located in the state of California.

77. At all times relevant to the allegations of this complaint, all of the activities complained of herein from which the ISP and CLEC gained profit as a partner with Adzilla took place by and through Adzilla's headquarters located in the state of California.

78. At all times relevant to the allegations of this complaint, Adzilla's ad network's conduct in altering the webpages viewed by consumers from the one that the website would ordinarily present, to the one that Adzilla's "re-engineered" for profit, was located in the state of California.

79. At all times relevant to the allegations of this complaint, on information and belief, all class members engaged in electronic communication on at least one occasion during the class period with servers were located in California. Such servers included, for example, the largest social network, Facebook, and two of the largest search engines, Google and Yahoo, each of which are located in the state of California. Thus, data sent from the host website based in California to the class member in their home state was subject to the interception and alteration as alleged in this complaint from actions taken in the state of California. Data sent from the subscriber to the host website based in California was subject to the interception for purposes of alteration in the state of California as alleged in this complaint.

80. At all times relevant to the allegations of this complaint, on information and belief, one or more business transactions and agreements between Adzilla and the ISPs and/or CLECs involved in the joint venture which forms the basis of this action occurred, in whole or part, in the state of California.

81. The geographic location from which the scheme to intercept, copy, obtain, analyze, store, and alter the data of internet subscribers was coordinated, launched, overseen, and implemented was the state of California.

82. The geographic location from which the interception, coping, obtaining, analyzing, storing, and altering of sensitive, financial, personal, private, and personally identifying information of internet subscribers was orchestrated and implemented in the state of California at Adzilla's California headquarters.

83. The actions of the ISP and the CLECs as described herein were not taken in a vacuum of ignorance, or lack of understanding as to the reason and motives for permitting the Zillacaster to be installed on their subscriber lines for purposes of collecting subscriber data. The ISP and the CLECs were motivated in their actions purely by profit, and knowingly and consciously aided, permitted, participated in, and profited by the secret monitoring of their internet subscribers, the collecting of their data, and the altering of their communications. Adzilla's own website unambiguously states:

> **What is the revenue opportunity?**
> The revenue sharing agreement will vary between ISPs. It is dependant on the location of the subscribers, the number of subscribers and the subscriber information provided by the ISP to the installed ZILLAcaster. The more targeted the information, the larger the revenue opportunity.

http://www.adzilla.com/Service_Provider_FAQ.pdf

Opting Out

84. In *no* case as alleged in this complaint, was adequate, informed notice provided to any class member of the true nature and function of the Adzilla service.

85. In *any* cases where *some* notice was provided, that notice was insufficient, misleading, and inadequate. Consent under such circumstances is impossible.

86. In *any* case where the opportunity of 'opting out' of the Adzilla service *was* provided, if at all, such 'opt out' rights were misleading, untrue, and deceptive.

87. 'Opting out,' if it was ever provided as an option to any person (which, in fact, it was not), only affected the provision of advertisements to the consumer who opted out (what the consumer saw). In no case was the collection of all internet communication data between the consumer and the internet halted or affected in any way. All data was still collected. The 'opt out' only affected what advertisements the consumer was shown. Thus, the provision of the opportunity for opting out was, itself, totally misleading.

Anonymization Of Data

88. The collection of data by the Adzilla device was wholesale and all-encompassing. All data passing though the hub was swept up without discrimination as to the kind, type, nature, or sensitivity of the data. Like a vacuum cleaner, everything passing through the pipe of the consumer's internet connection was sucked up, copied, and forwarded to the California processing center. Regardless of any representations to the contrary -- all data – whether sensitive, financial, personal, private, complete with all identifying information, and all personally identifying information, was recorded and transmitted to the California Adzilla facility.

CLASS ALLEGATIONS

Allegations as to Class Certification

89. Plaintiff bring this Complaint on behalf of herself and the following classes:

A) All AAISP Subscribers whose internet communications were monitored, intercepted, accessed, copied, transmitted, altered and/or used at any time by or through an Adzilla device.

and:

B) All AACLEC end-users whose internet communications were monitored, intercepted, accessed, copied, transmitted, altered and/or used at any time by or through an Adzilla device.

90. Additionally and/or alternatively, Plaintiff bring this Complaint on behalf of herself and the following subclasses:

i) All Core Communications, Inc. end-users whose internet communications were monitored, intercepted, accessed, copied, transmitted, altered and/or used at any time by or through an Adzilla device.

ii) All Continental VisiNet Broadband, Inc, subscribers whose internet communications were monitored, intercepted, accessed, copied, transmitted, altered and/or used at any time by or through an Adzilla device.

iii) All Doe AACLEC end-users whose internet communications were monitored, intercepted, accessed, copied, transmitted, altered and/or used at any time by or through an Adzilla device.

iv) All Doe AAISP subscribers whose internet communications were monitored, intercepted, accessed, copied, transmitted, altered and/or used

at any time by or through an Adzilla device.

91. Plaintiff reserve the right to revise these definitions of the classes based on facts she learns during discovery.

92. The classes are brought pursuant to Federal Rule of Civil Procedure 23 (the "Classes"). Excluded from the Classes are i) any Judge or Magistrate presiding over this action, and the court personnel supporting the Judge or Magistrate presiding over this action, and members of their respective families; ii) Defendants, Defendants' subsidiaries, parents, successors, predecessors, and any entity in which a Defendant or its parent has a controlling interest and their current or former employees, officers and directors; and iii) persons who properly execute and file a timely request for exclusion from the class and iv) the legal representatives, successors or assigns of any such excluded persons.

93. **Numerosity:** Individual joinder of all members of the Class is impracticable. The class and each subclass includes thousands of individuals. Upon information and belief, class members can be identified by the electronic records of defendants.

94. **Class Commonality:** Common questions of fact and law exist as to all Class members and predominate over the questions affecting only individual Class members. All class members were subscribers of one of the AAISPs or an end-user of a AACLEC during the time that the Zillacaster was engaged in the activities herein alleged. All class members' internet communications were monitored, intercepted, accessed, copied, transmitted, altered and/or used by defendants.

95. Common questions include:

a. What was the Adzilla device and how did it work?

b. What information did the Adzilla device collect and what did it do with that

information?

c. Was there proper notice, *or any notice*, of the operation of the Adzilla device to consumers?

d. Was there proper opportunity, *or any opportunity*, to decline the operation of the Adzilla device provided to consumers?

e. Whether AAISP subscribers, or AACLEC end-users, by virtue of their internet subscription, had pre-consented to the operation of the Adzilla device;

f. Whether AAISP subscribers, or AACLEC end-users, by virtue of their internet subscription, had consented at any time to the operation of the Adzilla device;

g. Did the operation, function, and/or implementation of the Adzilla device violate the ECPA?

h. Did the operation, function, and/or implementation of the Adzilla device violate California's Computer Crime Law, Cal. Penal Code § 502?

i. Did the operation, function, and/or implementation of the Adzilla device violate the Federal Computer Fraud And Abuse Act, 18 U.S.C. § 1030?

j. Did the operation, function, and/or implementation of the Adzilla device violate the Violation of the California Invasion of Privacy Act?

k. Did the Adzilla device transmit "personally identifying information?"

l. Did the operation, function, and/or implementation of the Adzilla device unjustly enrich the defendants herein?

m. Are the AAISPs and/or AACLECs liable under a theory of aiding and abetting, or conspiracy, for Adzilla's violations of the statutes listed herein?

n. Are class members entitled to damages as a result of the operation, function,

and/or implementation of the Adzilla device, and, if so, what is the measure of those damages?

o. Did the Adzilla device transmit "personally identifying information?"

p. The nature and extent of damages and other remedies to which the conduct of Defendants entitles the class members.

96. Defendants engaged in a common course of conduct giving rise to the legal rights sought to be enforced by the class members. Similar or identical statutory and common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison to the numerous common questions that dominate.

97. The injuries sustained by the class members flow, in each instance, from a common nucleus of operative facts. In each case, the Defendant AAISPs / AACLECs aided, permitted, participated in, and facilitated the monitoring, interception, access, coping, transmission, alteration and/or use of their private personal communications by or through the Adzilla device. Adzilla itself, installed and monitored, intercepted, accessed, copied, transmitted, altered and/or used said communications through the use of the Adzilla device without adequate notice, consent, or opportunity to opt out provided to the AAISP subscribers or AACLEC end-users.

98. **Typicality:** Plaintiff's claims are typical of the claims of other members of the Class, as the Plaintiff and other Class members were all subjected to Defendants' identical wrongful conduct based upon the same transactions which occurred uniformly to the Plaintiff and to the public.

99. **Adequacy**: Plaintiff will fairly and adequately protect the interests of the class. Plaintiff is familiar with the basic facts that form the bases of the proposed class members'

claims. Plaintiff's interests do not conflict with the interests of the other class members that she seeks to represent. Plaintiff has retained counsel competent and experienced in class action litigation and intend to prosecute this action vigorously. Plaintiff's counsel has successfully prosecuted complex actions including consumer protection class actions. Plaintiff and Plaintiff's counsel will fairly and adequately protect the interests of the class members.

100. **Superiority**: The class action device is superior to other available means for the fair and efficient adjudication of the claims of Plaintiff and the proposed class members. The relief sought per individual member of the class is small given the burden and expense of individual prosecution of the potentially extensive litigation necessitated by the conduct of Defendants. Furthermore, it would be virtually impossible for the class members to seek redress on an individual basis. Even if the class members herself could afford such individual litigation, the court system could not.

101. Individual litigation of the legal and factual issues raised by the conduct of Defendants would increase delay and expense to all parties and to the court system. The class action device presents far fewer management difficulties and provides the benefits of a single, uniform adjudication, economies of scale and comprehensive supervision by a single court.

102. Given the similar nature of the class members' claims and the absence of material differences in the state statutes and common laws upon which the class members' claims are based, a nationwide class will be easily managed by the Court and the parties.

103. The court may be requested to also incorporate subclasses of Plaintiffs, defendants, or both, in the interest of justice and judicial economy.

104. In the alternative, the class may be certified because:

a) the prosecution of separate actions by the individual members of the class would

create a risk of inconsistent or varying adjudication with respect to individual class members which would establish incompatible standards of conduct by defendant;

b) the prosecution of separate actions by individual class members would create a risk of adjudications with respect to them which would, as a practical matter, be dispositive of the interests of other class members not parties to the adjudications, or substantially impair or impede their ability to protect their interests; and

c) Defendants have acted or refused to act on grounds generally applicable to the class, thereby making appropriate final and injunctive relief with respect to the members of the class as a whole.

Count I:
VIOLATIONS OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT
Sections 2510 et seq.
(communications in transit)
Against All Defendants

105. Plaintiff incorporates the above allegations by reference as if set forth herein at length.

106. Plaintiff asserts this claim against each and every Defendant named herein in this complaint on behalf of herself and the Class.

107. This claim is alleged in addition to, or in the alternative to Count II, below, as to the AAISP and AACLEC defendants.

108. The federal Electronic Communications Privacy Act of 1986 ("ECPA", at 18 U.S.C. § 2511(1) makes it unlawful for a person to "willfully intercept[], endeavor[] to intercept, or procure[] any other person to intercept or endeavor to intercept, any wire, oral, or

electronic communication." 18 USC 2520(a) provides a civil cause of action to "any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of the ECPA.

109. The transmission of data by Plaintiff and the Class between their computers and the internet constitute “electronic communications” within the meaning of 18 U.S.C. §2510.

110. On information and belief, each of the Defendants have intentionally obtained and/or intercepted, by device or otherwise, these electronic communications without Plaintiff’s or Class members’ knowledge, consent, or authorization and while the communications were still en route.

111. On information and belief, each of the Defendants have procured another person or entity to intercept or endeavor to intercept, by device or otherwise, these electronic communications without Plaintiff’s or Class members’ knowledge, consent, or authorization and while the communications were still en route.

112. Defendants have intentionally used such electronic communications with knowledge or having reason to know that the electronic communications were obtained through interception for an unlawful purpose.

113. Defendants’ intentional interception of these electronic communications without Plaintiff’s or Class members’ knowledge, consent, or authorization was undertaken without a facially valid court order or certification.

114. Defendants intentionally acquired and/or intercepted the contents of electronic communications sent by and/or received by Plaintiff through the use of an electronic device. Defendants intentionally acquired the communications that had been sent from or directed to Plaintiff through their use of computers and other electronic devices which were part of, and

utilized in, Defendants' electronic communications system, in violation of 18 U.S.C. § 2511 and pursuant to 18 U.S.C. § 2520.

115. Defendants unlawfully accessed and used, and voluntarily disclosed, the contents of the intercepted communications to enhance their profitability and revenue through advertising. This disclosure was not necessary for the operation of Defendants' system or to protect Defendants' rights or property.

116. Plaintiff is "person[s] whose … electronic communication is intercepted … or intentionally used in violation of this chapter" within the meaning of 18 U.S.C. § 2520.

117. Defendants, and each of them, are liable directly for this cause of action. Plaintiff therefore seek remedy as provided for by 18 U.S.C. § 2520, including such preliminary and other equitable or declaratory relief as may be appropriate, damages consistent with subsection (c) of that section to be proven at trial, punitive damages to be proven at trial, and reasonable attorney's fees and other litigation costs reasonably incurred.

118. Plaintiff and the Class, pursuant to 18 U.S.C. §2520, are entitled to preliminary, equitable, and declaratory relief, in addition to statutory damages of the greater of $10,000 or $100 a day for each day of violation, actual and punitive damages, reasonable attorneys' fees, and Defendants' profits obtained from the above-described violations.

Count II:
VIOLATIONS OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT
Sections 2701 et seq.
(communications in storage)
Against Continental Broadband and CorTel and John Does 1-50
("AAISP / AACLEC Defendants")

119. Plaintiff incorporates the above allegations by reference as if set forth herein at length.

120. Plaintiff asserts this claim against each and every Defendant named herein in this complaint on behalf of herself and the Class.

121. This claim is alleged in addition to, or in the alternative to Count I, above as to the AAISP and AACLEC Defendants.

122. The federal Electronic Communications Privacy Act of 1986 ("ECPA", at 18 U.S.C. § 2702(a)(2) makes it unlawful for a person to “knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service . . . (A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service.”

123. 18 USC 2707 (a) provides a civil cause of action to "any person aggrieved by any violation of this chapter.”

124. The transmission of data by Plaintiff and the Class between their computers and the internet constitute “electronic communications” within the meaning of 18 U.S.C. §2510.

125. On information and belief, each of the Defendants have knowingly accessed, obtained, divulged, and/or altered electronic communications of Plaintiff and the class while such communications were in temporary storage of the defendant, either for subsequent transmission to its destination, or for backup purposes, or otherwise temporarily stored, without Plaintiff’s or Class members’ knowledge, consent, or authorization.

126. On information and belief, each of the Defendants have knowingly accessed, obtained, divulged, and/or altered electronic communications of Plaintiff and the class while such communications were in temporary storage of the defendant in excess of any authorization provided by Plaintiff’s or members of the Class.

127. Defendant intentionally accessed, obtained, divulged, and/or altered electronic communications of Plaintiff and the class with knowledge or having reason to know that the electronic communications were obtained through unlawful means and for an unlawful purpose.

128. Defendants intentionally accessed, obtained, divulged, and/or altered electronic communications of Plaintiff and the class with knowledge or having reason to know that the electronic communications were obtained without a facially valid court order or certification.

129. Defendants intentionally accessed, obtained, divulged, and/or altered electronic communications of Plaintiff and the class with knowledge or having reason to know that the electronic communications were obtained to enhance their profitability and revenue through advertising. These actions were not necessary for the operation of Defendants' system or to protect Defendants' rights or property.

130. Defendants intentionally accessed, obtained, divulged, and/or altered electronic communications of Plaintiff and the class with knowledge or having reason to know that the electronic communications obtained were not divulged in order to forward such communications to their destination.

131. Defendants intentionally accessed, obtained, divulged, and/or altered electronic communications of Plaintiff and the class with knowledge or having reason to know that the electronic communications obtained were not necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service.

132. Defendants, and each of them, are liable directly for this cause of action. Plaintiff therefore seek remedy as provided for by 18 U.S.C. § 2707, including such preliminary and other equitable or declaratory relief as may be appropriate, damages consistent with

subsection (c) of that section to be proven at trial, punitive damages to be proven at trial, and reasonable attorney's fees and other litigation costs reasonably incurred.

133. Plaintiff and the Class, pursuant to 18 U.S.C. §2707, are entitled to preliminary, equitable, and declaratory relief, in addition to statutory damages of a minimum of $1,000 for each violation, actual and punitive damages, reasonable attorneys' fees, and Defendants' profits obtained from the above-described violations.

Count III
VIOLATION OF CALIFORNIA'S COMPUTER CRIME LAW
CAL. PENAL CODE § 502
Against All Defendants

134. Plaintiff incorporates the above allegations by reference as if set forth herein at length.

135. Plaintiff asserts this claim against each and every Defendant named herein in this complaint on behalf of herself and the Class.

136. Defendants accessed, copied, used, made use of, interfered, and/or altered, data belonging to class members: (1) in and from the State of California; (2) in the home states of the plaintiffs; and (3) in the state in which the servers that provided the communication link between Plaintiff and the websites they interacted with were located.

137. Cal. Penal Code § 502(j) states: "For purposes of bringing a civil or a criminal action under this section, a person who causes, by any means, the access of a computer, computer system, or computer network in one jurisdiction from another jurisdiction is deemed to have personally accessed the computer, computer system, or computer network in each jurisdiction.

138. Defendants have violated California Penal Code § 502(c)(1) by knowingly and without permission, altering, and making use of data from Plaintiff's computers in order to

wrongfully obtain valuable private data from Plaintiffs.

139. Defendants have violated California Penal Code § 502(c)(1) by knowingly and without permission, altering, and making use of data from Plaintiff's computers in order to: (1) deceive Plaintiff into surrendering private internet communications and activities for defendants' financial gain; and (2) deceive Plaintiff into accepting and clicking on ads of defendant's creation instead of the ads proffered by the websites they were interacting with, including websites of financial institutions, business concerns, governmental agencies, and others within California.

140. Defendants have violated California Penal Code § 502(c)(2) by knowingly and without permission, accessing and taking data from Plaintiff computers.

141. Defendants have violated California Penal Code § 502(c)(4) by knowingly and without permission, adding and/or altering the data that appeared upon Plaintiff's computers.

142. Defendants have violated California Penal Code § 502(c)(6) by knowingly and without permission providing, or assisting in providing, a means of accessing Plaintiff's computers, computer system, and/or computer network.

143. Defendants have violated California Penal Code § 502(c)(7) by knowingly and without permission accessing, or causing to be accessed, Plaintiff's computer system, and/or computer network.

144. Pursuant to California Penal Code § 502(b)(10) a "Computer contaminant" means any set of computer instructions that are designed to . . . record, or transmit information within a computer, computer system, or computer network without the intent or permission of the owner of the information.

145. Defendants have violated California Penal Code § 502(c)(8) by knowingly and without permission introducing a computer contaminant into the transactions between Plaintiff and defendants.

146. As a direct and proximate result of Defendants' unlawful conduct within the meaning of California Penal Code § 502, Defendants have caused loss to Plaintiff in an amount to be proven at trial. Plaintiff is also entitled to recover their reasonable attorneys' fees pursuant to California Penal Code § 502(e).

147. Plaintiff has also suffered irreparable injury from these unauthorized acts of disclosure, to wit: all of their personal, private, and sensitive web communications have been harvested, viewed, accessed, stored, and used by Defendants, and have not been destroyed, and, due to the continuing threat of such injury, plaintiff has no adequate remedy at law, entitling Plaintiff to injunctive relief.

Count IV
VIOLATION OF FEDERAL COMPUTER FRAUD AND ABUSE ACT
18 U.S.C. § 1030
Against Defendants Conducive and Adzilla

148. Plaintiff incorporates the above allegations by reference as if set forth herein at length.

149. Plaintiff asserts this claim against each and every Defendant named herein in this complaint on behalf of herself and the Class.

150. On information and belief, during the class period, Plaintiff and members of the class, routinely accessed the websites of "financial institutions" as that term is defined in 18 U.S.C. § 1030(e)(4), and/or "governmental entities" as that term is defined in 18 U.S.C. § 1030(e)(9). Such access included the input, transmission, and receipt of access codes,

passwords, and financial data all comprising "financial records" as that term is defined in 18 U.S.C. § 1030(e)(5).

151. By virtue of the access of Plaintiff and members of the class to the computers of "financial institutions" and/or "governmental entities" Defendants, and each of them, gained access to "protected computers" as that term is defined in 18 U.S.C. § 1030(e)(2).

152. The information that the Zillacaster collected has value in the marketplace. In fact, the information collected by the Zillacaster was so valuable, that Adzilla offered to pay, and, in fact, on information and belief, did pay to the AACLECs and to the AAISPs substantial sums of money in exchange for collecting and the opportunity to exploit that data.

153. The data collected by the Zillacaster was private, personal information which belonged to Plaintiff and members of the class. The private personal data of Plaintiff and class members is capable of valuation and monetization in the marketplace. Marketing companies pay or otherwise compensate consumers for the provision of the type of data that was collected by the Zillacaster.

154. Plaintiff and members of the class suffered damage when their personal private and confidential data, which has a value in the marketplace, was taken from them without their consent and without any compensation whatsoever.

155. Plaintiff and members of the class suffered loss of revenue when their personal private and confidential data, which has a value in the marketplace, was taken from them without their consent and without any compensation whatsoever.

156. As a result of this uncompensated taking of private, personal data from Plaintiff and members of the class, Defendants' conduct has caused a loss to one or more persons during any one-year period aggregating at least $5,000 in value in real economic damages.

157. Plaintiff have additionally suffered loss by reason of these violations, including, without limitation, violation of the right of privacy, disclosure of affiliation and business relationships between Plaintiff and internet product and service providers, and disclosure of specific purchase and transactional information that otherwise is private, confidential, and not of public record.

158. Defendants' unlawful access to Plaintiff's computers and computer communications also have caused Plaintiff irreparable injury. Unless restrained and enjoined, Defendants will continue to commit such acts. Plaintiff's remedy at law is not adequate to compensate it for these inflicted and threatened injuries, entitling Plaintiff to remedies including injunctive relief as provided by 18 U.S.C. § 1030(g).

Count V
VIOLATION OF THE CALIFORNIA INVASION OF PRIVACY ACT,
Penal Code Section 630 et seq.
Against All Defendants

159. Plaintiff incorporates the above allegations by reference as if set forth herein at length.

160. Plaintiff asserts this claim against each and every Defendant named herein in this complaint on behalf of herself and the Class.

161. California Penal Code section 630 provides, in part:

> Any person who, . . . or who willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section, is punishable . . .

162. On information and belief, the Plaintiff, and each class member, during one or more of their interactions on the internet during the class period, communicated with one or more web entities based in California, or with one or more entities whose servers were located in California, or communicated by email with persons or entities located in California.

163. Communications from the California web-based persons or entities to Plaintiff and class members were sent *from* California. Communications to the California web-based persons or entities from Plaintiff and class members were sent *to* California.

164. Plaintiff and class members did not consent to Adzilla's nor any of the AAISPs / AACLECs actions in intercepting, reading, and/or learning the contents of their communications with such California-based persons or entities.

165. Plaintiff and class members did not consent to Adzilla's nor any of the AAISPs / AACLECs actions in using the contents of their communications with such California-based persons or entities.

166. Adzilla is not a " public utility engaged in the business of providing communications services and facilities . . ."

167. The actions alleged herein by the Defendant AAISPs / AACLECs were not undertaken: "for the purpose of construction, maintenance, conduct or operation of the services and facilities of the public utility."

168. The actions alleged herein by the Defendant AAISPs / AACLECs were not undertaken in connection with: "the use of any instrument, equipment, facility, or service furnished and used pursuant to the tariffs of a public utility.

169. The actions alleged herein by the Defendant AAISPs / AACLECs were not undertaken with respect to any telephonic communication system used for communication exclusively within a state, county, city and county, or city correctional facility.

170. The Defendant AAISPs / AACLECs directly participated in the interception, reading, and/or learning the contents of the communications between plaintiffs, class members and California-based web entities.

171. Alternatively, and of equal violation of the California Invasion of Privacy Act, the Defendant AAISPs / AACLECs aided, agreed with, and/or conspired with Adzilla to unlawfully do, or permit, or cause to be done all of the acts complained of herein.

172. Pursuant to Section 637.2 of the California Penal Code, Plaintiff and the class have been injured by the violations of California Penal Code section 631. Wherefore, plaintiffs, on behalf of herself and on behalf of a similarly situated Class of consumers, seek damages and injunctive relief.

Count VI:
AIDING AND ABETTING VIOLATIONS OF:
--California's Computer Crime Law Cal. Penal Code § 502; and
--The Federal Computer Fraud and Abuse Act 18 U.S.C. § 1030; and
--The California Invasion of Privacy Act
Against Continental Broadband and CoreTel and John Does 1-50
("AAISP / AACLEC Defendants")

173. Plaintiff incorporates the above allegations by reference as if set forth herein at length.

174. As fully described above, The AAISP / AACLEC Defendants had full knowledge or should have reasonably known of the true nature of the wrongful conduct conducted by Adzilla.

175. The AAISP / AACLEC Defendants knew that, through the implementation of

Adzilla's Deep Packet Inspection of its subscribers' internet communications, Adzilla would, in real time, receive personally identifying information along with sensitive, financial, personal, private, information unknowingly transmitted and communicated by its subscribers who had no adequate notice that their communications were being intercepted, all in violation of California's Computer Crime Law Cal. Penal Code § 502; the Federal Computer Fraud And Abuse Act 18 U.S.C. § 1030; and California's Invasion of Privacy Act.

176. The AAISP / AACLEC Defendants aided and abetted such wrongful conduct, including providing the means and the access to violate these state and federal statutes.

177. The AAISP / AACLEC Defendants knew, or should have known, that the conduct Adzilla engaged in by use of Deep Packet Inspection of its subscribers' data transmissions and communications was unlawful and that the AAISP's provision of access to their subscribers' internet communications was the means by which that unlawful conduct took place.

178. The AAISP / AACLEC Defendants knew, or should have known, at all relevant times herein, of their role as part of an overall illegal or tortious activity at the time that the AAISPs / AACLECs provided their assistance.

179. As a direct and proximate result of the aiding and abetting of these acts, Plaintiff and the class have suffered injury and harm and loss, including, but not limited to, loss of the user's privacy with respect to their actions on the internet (where class members shop, what they buy and look at, where they browse, and what goods and services they seek), loss of privacy with respect to their associational relationships on the internet); and loss of privacy with respect to their interests, hobbies, and activities on the internet. The wrongful conduct aided and abetted by the AAISP / AACLEC Defendants was a substantial factor in causing this harm.

180. The AAISP / AACLEC Defendants' intentional aiding and abetting to commit, and commission of, these wrongful acts was willful, malicious, oppressive, and in conscious disregard of the rights of Plaintiff and the class, and Plaintiff and the class are therefore entitled to an award of punitive damages to punish the wrongful conduct of Defendants and deter future wrongful conduct.

Count VII
CIVIL CONSPIRACY ON BEHALF OF THE CLASS
Against Continental Broadband and CoreTel and John Does 1-50
("AAISP / AACLEC Defendants")

181. Plaintiff incorporate the above allegations by reference as if set forth herein at length.

182. The AAISP / AACLEC Defendants willfully, intentionally, and knowingly agreed and conspired with Adzilla to engage in the alleged wrongful conduct, including Adzilla's violations of California's Computer Crime Law Cal. Penal Code § 502, the Federal Computer Fraud And Abuse Act 18 U.S.C. § 1030, and California's Invasion of Privacy Act.

183. The AAISP / AACLEC Defendants did the acts alleged herein pursuant to, and in furtherance of, that agreement and/or furthered the conspiracy by cooperating, encouraging, ratifying, or adopting the acts of the others.

184. As a direct and proximate result of the aiding and abetting of these acts, Plaintiff has suffered injury and harm and loss, including, but not limited to, loss of the user's privacy with respect to their actions on the internet (where class members shop, what they buy and look at, where they browse, and what goods and services they seek), loss of privacy with respect to their associational relationships on the internet); and loss of privacy with respect to their interests, hobbies, and activities on the internet.

185. The wrongful conduct committed pursuant to the conspiracy was a substantial

factor in causing this harm.

186. The AAISP / AACLEC Defendants' intentional agreement to commit, and commission of, these wrongful acts was willful, malicious, oppressive, and in conscious disregard of the rights of Plaintiff and the class, and Plaintiff and the class are therefore entitled to an award of punitive damages to punish the wrongful conduct of Defendants and deter future wrongful conduct.

Count VIII
Unjust Enrichment
Against All Defendants

187. Plaintiff incorporates by reference the foregoing allegations.

188. Plaintiff asserts this claim against each and every Defendant named herein in this complaint on behalf of herself and the Class.

189. A benefit has been conferred upon all Defendants by Plaintiff and the Class. On information and belief, Defendants, directly or indirectly, have received and retain information regarding communications between Plaintiff and internet product and service providers, and have received and retain information regarding specific purchase and transactional information that is otherwise private, confidential, and not of public record, and/or have received revenue from the provision of such information.

190. Defendants appreciate or have knowledge of said benefit.

191. Under principles of equity and good conscience, Defendants should not be permitted to retain the information and/or revenue which they acquired by virtue of their unlawful conduct. All funds, revenues, and benefits received by Defendants rightfully belong to Plaintiff and the Class, which Defendants have unjustly received as a result of their actions.

Prayer for Relief

WHEREFORE, Plaintiff respectfully pray for the following:

a) With respect to all counts, declaring the action to be a proper class action and designating Plaintiff and their counsel as representatives of the Class;

b) As applicable to the Class *mutatis mutandis*, awarding injunctive and equitable relief including, *inter alia*: (i) prohibiting Defendants from engaging in the acts alleged above; (ii) requiring Defendants to disgorge all of their ill-gotten gains to Plaintiff and the other Class members, or to whomever the Court deems appropriate; (iii) requiring Defendants to delete all data surreptitiously or otherwise collected through the acts alleged above; (iv) requiring Defendants to provide Plaintiff and the other class members a means to easily and permanently decline any participation in any data collection activities by means of the Adzilla device or any similar device, in any present or future iteration of the Adzilla device; (v) awarding Plaintiff and class members full restitution of all benefits wrongfully acquired by Defendants by means of the wrongful conduct alleged herein; and (vi) ordering an accounting and constructive trust imposed on the data, funds, or other assets obtained by unlawful means as alleged above, to avoid dissipation, fraudulent transfers, and/or concealment of such assets by Defendants;

c) For a preliminary and permanent injunction restraining Defendants, their officers, agents, servants, employees, and attorneys, and those in active concert or participation with any of them from:

(1) transmitting any information about Plaintiff or class member's activities on the internet for advertising purposes to any other websites,

without fair, clear and conspicuous notice of the intent to transmit information, including a full description of all information potentially and/or actually available for transmission;

(2) transmitting any information about Plaintiff or class member's activities on the internet for advertising purposes to any other websites, without fair, clear and conspicuous opportunity to decline the transmittal prior to any transmission of data or information;

d) Awarding damages, including statutory damages where applicable, to the Class in an amount to be determined at trial;

e) Awarding Plaintiff reasonable attorney's fees and costs;

f) Awarding pre- and post-judgment interest; and

g) Granting such other and further relief as the Court may deem just and proper.

JURY TRIAL DEMAND

The Plaintiff hereby demands a trial by jury of all issues so triable.

Respectfully submitted,

DATED this 27th day of February, 2009.

By: Alan Himmelfarb

Alan Himmelfarb
KamberEdelson, LLC
2757 Leonis Blvd.
Vernon, California 90058-2304
Telephone: (323) 585-8696
ahimmelfarb@kamberedelson.com

Scott A. Kamber
KamberEdelson, LLC
11 Broadway, 22nd Floor.

New York, NY. 10004
Telephone: (212) 920-3072
Fax: (212) 202-6364
skamber@kamberedelson.com *(Pro Hac Vice Pending)*

Joseph H. Malley
Law Office of Joseph H. Malley
1045 North Zang Boulevard
Dallas, Texas 75208
Ph. (214) 943-6100
Fax (214) 943-6170
malleylaw@gmail.com *(Pro Hac Vice Pending)*